

02/11/00
JC580 U.S. PTO

Atty. Docket No. RSW9-99-129

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application Transmittal

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is the **Patent Application** of:

Inventor: K. S. Attwood, et al

For: Technique of Defending Against Network Connection Flooding Attacks

Enclosed are:



2 sheets of drawings.



An assignment of the invention to International Business Machines Corporation, Armonk, New York 10504.



A certified copy of a _____ application.



An associate power of attorney.



Declaration and Power of Attorney for Patent Application

The filing fee has been calculated as shown below:

(Col. 1)

(Col. 2)

Other Than Small Entity

For:	No. Filed	No. Extra
Basic Fee		
Total Claims	16-20 =	0
Indep. Claims	4-3 =	1
<input checked="" type="checkbox"/> Multiple Dependent Claim Presented		

Rate	Fee
	\$690.00
x \$18.00=	\$.00
x \$78.00=	\$78.00
\$260.00	\$260.00
Subtotal	\$1028.00
\$130.00	\$.00
TOTAL	\$1028.00

Surcharge-Late Filing Fee or Oath or Declaration

Deposit Account Authorization



Please charge Deposit Account No. 09-0461 in the amount of \$1028.00. A duplicate copy of this sheet is enclosed.



The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 09-0461. A duplicate copy of this sheet is enclosed.



Any additional filing fees required under 37 C.F.R. §1.16.



Any patent application processing fees under 37 C.F.R. §1.17.

Date: February 11, 2000

Respectfully submitted,

By

Jerry W. Herndon
Attorney of Record
Registration No. 27,901
IBM Corporation
Intellectual Property Law
Dept. T81/Bldg. 062
P.O. Box 12195
Research Triangle Park, NC 27709
Telephone: 919- 543-3754
Fax: 919-254-4330

EXPRESS MAIL CERTIFICATE

Express Mail Label
Number: EJ922477644US
Date: February 11, 2000

I hereby certify that I am depositing the enclosed or attached paper with the U.S. Postal Service "Express Mail Post Office to Addressee" service on the above date, addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231.

Jennifer Dianne Lane

EXPRESS MAIL LABEL NO.: EJ922477644US DATE OF DEPOSIT: 2/11/2000
I hereby certify that this paper and fee are being deposited with the United States Postal Service
Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and
is addressed to the Assistant Commissioner of Patents, Washington, D.C. 20231.
Jennifer Dianne Lane
NAME OF PERSON MAILING PAPER AND FEE SIGNATURE OF PERSON MAILING PAPER AND FEE

INVENTORS: K. Attwood, L. Overby, J. Sun

Technique of Defending Against Network Connection Flooding Attacks

Technical Field

The invention relates generally to the field of networking and specifically to defending against attacks by malicious users attempting to disable a server by flooding the server with network traffic.

Background of the Invention

Flooding attacks have recently been used with increasing frequency to target and disable servers on the Internet. A flooding attack occurs when a user sends a large number of requests to a server in a relatively short period

of time with an intent to overload and thereby disable the server. A flood of packets from a malicious user can overload a server in the same way that a flood of packets from a misconfigured system can overload a server. But the end result is the same; the server becomes overloaded in trying to service the requests. This prevents legitimate requests from being timely served and often disables a server or causes it to crash. A number of flooding attacks have been reported in the news recently on well known web targets. Flooding attacks are very difficult for traditional intrusion detection systems to prevent due to the difficulty of determining whether traffic is legitimate or not.

Summary of the Invention

The invention recognizes that the consequences of intentional flooding attacks and unintentional overload situations resulting from a burst of connection requests can be mitigated by dropping the traditional notion of attempting to distinguish between legitimate and illegitimate traffic. In the invention, all traffic is subject to a policy that attempts to guarantee that legitimate work will be performed and a server will not crash in flooding situations, irrespective of whether the flooding is caused by legitimate or illegitimate traffic.

The invention helps to prevent a server from crashing due to

overload and it prevents one or more attackers from consuming all server resources.

5 In response to a request from a host for a connection to a port number on a server, the number of connections to the port that are assigned to the host are determined. If this number exceeds a first threshold, the request for a connection is denied. In the preferred embodiment, it is possible to override a decision to deny a connection request if a quality of service parameter pertaining to the
10 requesting host permits such an override. However, in the preferred embodiment, if the number of available connections to the port is less than a second threshold, the connection request is denied in any event. The denial of connections to a given host mitigate the effects of intentional or
15 unintentional bursts of connection requests. The overriding of a decision to deny a given request based on a quality of service parameter specific to a requesting host helps in meeting service guarantees that may have been made to a specific host. However, even in the presence of overriding
20 quality of service parameters, the denial of a connection when the number of available port connections becomes prohibitively small helps to prevent the complete disablement of a server.

25 In the preferred embodiment, the owner of a server specifies for each port number that is subject to flooding checks a maximum number of connections (M) allowed at any

time to the port and a controlling percentage (P) of
unassigned (available) connections remaining for the port.
The invention keeps track of the number of assigned
(unavailable) connections to a port and it calculates the
5 number of available port connections by subtracting the
number of unavailable connections from the maximum number of
connections. The percentage P is used to establish the
first threshold to trigger the initial decision to deny a
connection request. Specifically, the initial denial is
10 triggered if the existing number of connections assigned to
the requesting host is equal to or greater than the
threshold percentage of the available connections.

The maximum number of connections and the thresholds
will be difficult for most owners to configure. Therefore, a
"statistics" mode is provided that measures normal traffic
15 loads of different servers and suggests appropriate maximums
and thresholds that will not hamper similar legitimate
traffic loads. This statistics mode is not part of the
claimed invention and is not described further herein.

20 A similar technique can be applied to connectionless
traffic, such as UDP datagrams. This is the subject matter
of patent application number ____.

Brief Description of the Drawing

In the drawing:

5 Figs. 1 and 2 show an illustrative flowchart of operations executed at a server in response to the receipt of a request for connection to a port to ensure that flooding connection requests do not prevent the completion of other work and do not crash the server.

Detailed Description

10 The invention requires that an owner of a server using the invention configure the server with certain parameters. By way of example, the preferred embodiment requires that the owner specify for each port number subject to flooding checks a maximum number of connections (M) allowed at any time to the port and a threshold percentage (P) of available connections remaining for the port. The percentage P of 15 available connections for a port establishes a first threshold that triggers the denial of a connection request. As connections are assigned and released, the server maintains the number of connections assigned to each host 20 for each port. The server can therefore dynamically calculate the number of available connections for a port at the time a new request is received from the specified maximum number and the number of connections already

assigned to the port.

An entry is made to step 100 in Fig. 1 when a TCP/SYN request for a connection is first received at a network server. A SYN request is the first handshake of a three-flow protocol conventionally required to establish a TCP connection. At step 102, an acknowledgment to the TCP/SYN request is returned by the server to the host requesting a connection. At step 104, the requesting host returns a TCP acknowledgment. This completes the handshake protocol.

Step 106 determines the port number to which the request is directed from the requesting host acknowledgment. In TCP, a port number represents a destination within a given host computer to which a connection is requested. Some ports are reserved for standard services. For example, convention specifies that port 21 is used by the File Transport Protocol (FTP). The identity (the IP address) of the requesting host is also determined during the handshake protocol. The port number is used by step 108 to locate a memory control block for the port or to create one if a port control block does not exist. Attached to the port control block are a plurality of host control blocks for hosts that presently have one or more active connections. If the requesting host does not have a host control block, one is created. A host control block contains, among other things, a count of the port connections presently assigned to the host.

At step 110, the server fetches the maximum number of connections M specified for this port number, the controlling percentage P and the number A of active connections. Step 112 calculates the number I of available connections as $M - A$. Step 114 determines if the number of connections already assigned to the requesting host is equal to or greater than P times I. If so, then the connection request will be denied unless certain other precautions override the denial. On the other hand, if the number of connections already assigned to the requesting host is less than P times I, the connection request is allowed at step 116 and A is incremented by one to update the number of connections active to this port number.

Connection point A in Fig. 2 is entered from step 114 if the number of connections already assigned to the requesting host is equal to or greater than P times I. Step 202 first determines if the port is in a constrained state. A port is in a constrained state if the number of idle connections remaining on the port is equal to or less than some percentage X of the maximum number M of connections allowed to the port. X is 10 percent in the preferred embodiment. If this is true, the connection request is rejected at step 208. However, if the port is not constrained, then a Quality of Service (QOS) specification that pertains specifically to the requesting host can override the decision to reject the connection. In this

case, the request might be allowed at step 206, in which case the parameter A is updated by incrementing it by one. In other words, steps 202, 204 and 206 in conjunction implement a policy that rejects a connection request, unless
5 a QOS policy pertaining to the requester overrides the denial. But, if the requested port is in a constrained state, meaning that only a small number of connections remain to the port, the request is denied in any event.

The computer program that has been described can be executed on virtually any type of computer, ranging from personal computers to large mainframes such as IBM's System 390 machines. The only requirement is that the computer is configured with network communication software and is accessible as a server via a network.

Skilled artisans in the fields to which the invention pertains will recognize that numerous variations can be made to the embodiments disclosed herein and still remain within the sprit and scope of the invention.

What is Claimed:

1 1. A method of preventing a flooding attack on a network
2 server in which a large number of requests are received for
3 connection to a port number on the server, comprising:

4 determining, in response to a request from a host for a
5 connection to a port number on the server, if the number of
6 connections to the port assigned to the host exceeds a
7 prescribed threshold, and, if so,

8 denying the request for a connection.

9 2. The method of claim 1 in which denying the request
10 further comprises:

11 overriding the denial and allowing the request if a
12 quality of service parameter pertaining to the requesting
13 host permits the override.

14 3. The method of claim 2 wherein a connection request is
15 denied in any event if the number of available connections
16 to the port are less than a constrained threshold.

17 4. The method of claim 1 or claim 2 or claim 3 further
18 comprising:

calculating the prescribed threshold by multiplying a percentage P by the number of available connections remaining for the port.

5. Apparatus for preventing a flooding attack on a network server in which a large number of requests are received for connection to a port number on the server, comprising:

means for determining, in response to a request from a host for a connection to a port number on the server, if the number of connections to the port assigned to the host exceeds a prescribed threshold, and

means responsive to the determining means for denying the request for a connection.

6. The apparatus of claim 5 in which means for denying further comprises:

means responsive to a quality of service parameter pertaining to the requesting host for overriding a request denial and allowing the request.

7. The apparatus of claim 6 further comprising:

means for denying a connection request in any event if the number of available connections to the port are less

4 than a constrained threshold.

1 8. The apparatus of claim 5 or claim 6 or claim 7 further
2 comprising:

3 means for calculating the prescribed threshold by
4 multiplying a percentage P by the number of available
5 connections remaining for the port.

1 9. A storage media containing program code segments for
2 preventing a flooding attack on a network server in which a
3 large number of requests are received for connection to a
4 port number on the server, comprising:

5 a first code segment activated in response to a request
6 from a host for a connection to a port number on the server
7 for determining if the number of connections to the port
8 assigned to the host exceeds a prescribed threshold, and

9 a second code segment responsive to the first code
10 segment for denying the request for a connection.

1 10. The media of claim 9 in which the second code segment
2 further comprises:

3 a third code segment for overriding the denial and
4 allowing the request if a quality of service parameter

5 pertaining to the requesting host permits the override.

1 11. The media of claim 10 further comprising a fourth code
2 segment for denying a connection request in any event if the
3 number of available connections to the port are less than a
4 constrained threshold.

1 12 . The media of claim 9 or claim 10 or claim 11 further
2 comprising:

3 a fifth code segment for calculating the prescribed
4 threshold by multiplying a percentage P by the number of
5 available connections remaining for the port.

1 13. A carrier wave containing program code segments for
2 preventing a flooding attack on a network server in which a
3 large number of requests are received for connection to a
4 port number on the server, comprising:

5 a first code segment activated in response to a request
6 from a host for a connection to a port number on the server
7 for determining if the number of connections to the port
8 assigned to the host exceeds a prescribed threshold, and

9 a second code segment responsive to the first code
10 segment for denying the request for a connection.

1 14. The carrier wave of claim 13 in which the second code
2 segment further comprises:

3 a third code segment for overriding the denial and
4 allowing the request if a quality of service parameter
5 pertaining to the requesting host permits the override.

1 15. The carrier wave of claim 14 further comprising a
2 fourth code segment for denying a connection request in any
3 event if the number of available connections to the port are
4 less than a constrained threshold.

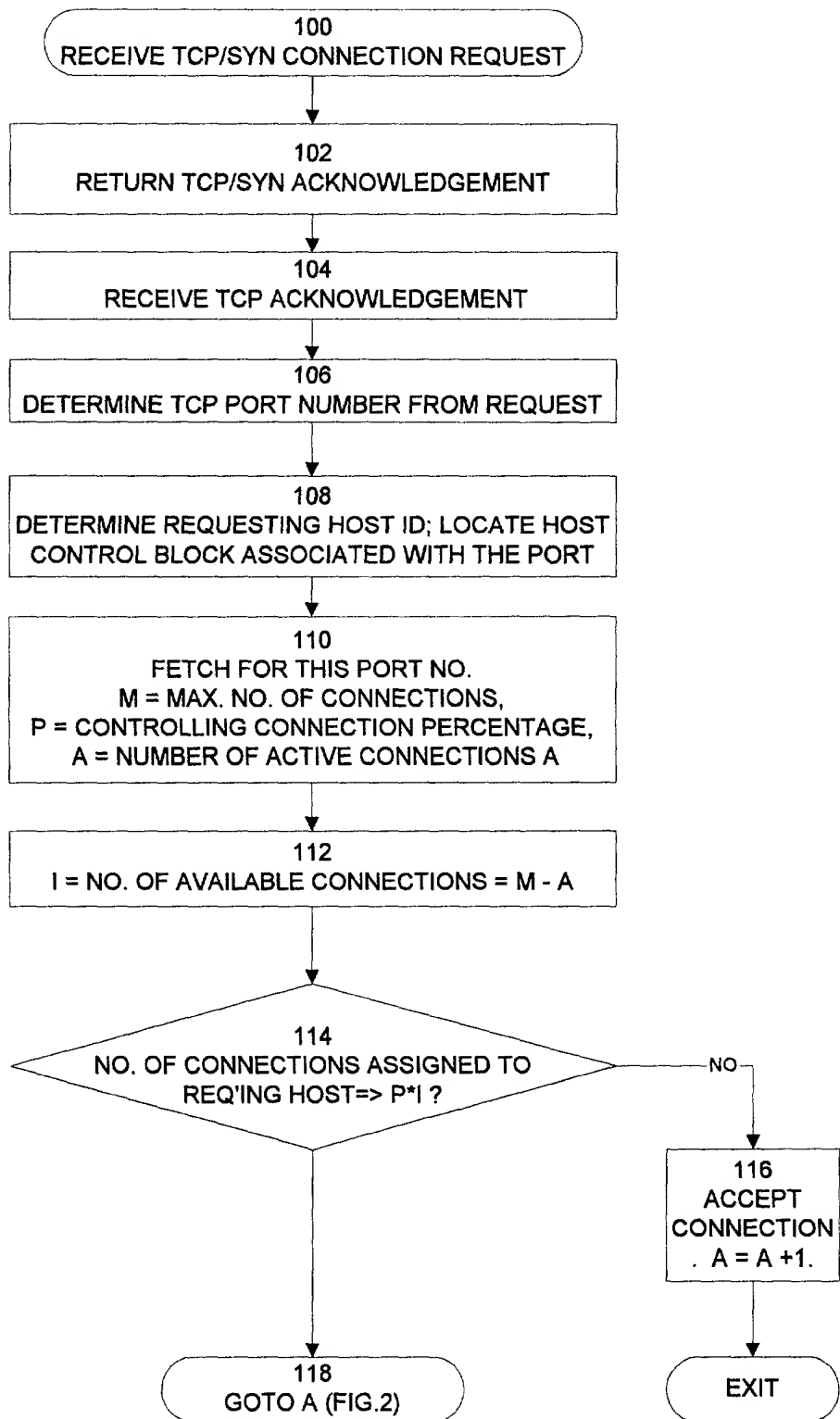
1 16. The carrier wave of claim 13 or claim 14 or claim 15
2 further comprising:

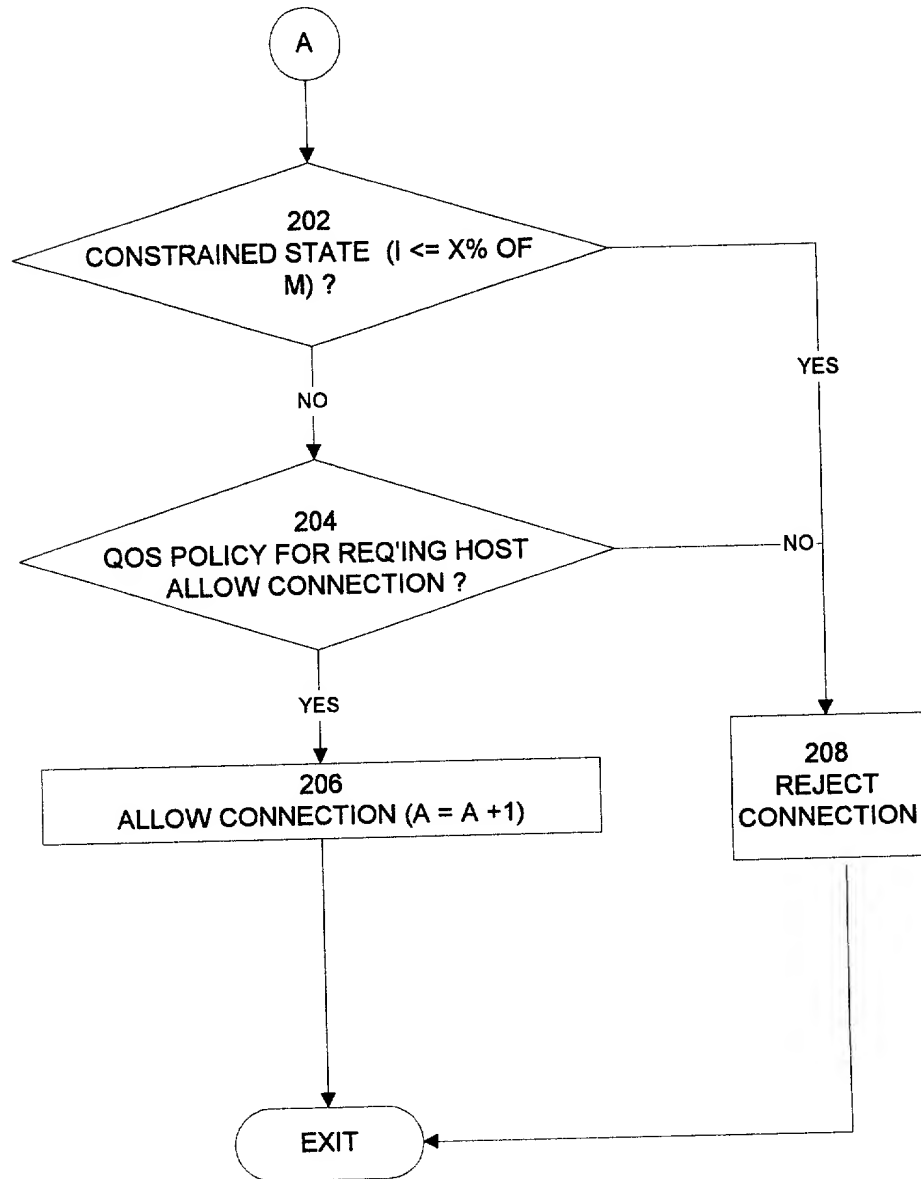
3 a fifth code segment for calculating the prescribed
4 threshold by multiplying a percentage P by the number of
5 available connections remaining for the port.

Technique of Defending Against Network Connection Flooding Attacks

5 The invention prevents server overload and possible
server crippling due to a flooding of connect requests
caused by intentional attack or otherwise. In response to a
connection request from a host for a specified port, the
number of connections to the port that are assigned to the
host are determined. If this number exceeds a first
10 threshold, the request is denied. It is possible to
override this denial if a quality of service parameter
pertaining to the host permits such an override. However,
if the number of available connections to the port is less
than a second threshold, the connection request is denied in
15 any event.

FIG. 1





Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

TECHNIQUE OF DEFENDING AGAINST NETWORK CONNECTION FLOODING ATTACKS

the specification of which (check one)



is attached hereto.



was filed on _____ as Application Serial No. _____.

I hereby state that I have reviewed and understand the contents of the above- identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

Number

Country

Day/Month/Year

Priority Claimed

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Applications:

Serial No.

Filing Date

Status

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

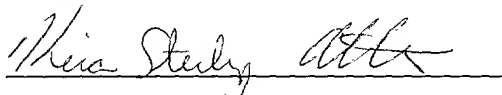
As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

A.B. Clay, Reg. No. 32,121; G. M. Doudnikoff, Reg. No. 32,847; E. H. Duffield, Reg. No. 25,970;
J. W. Herndon, Reg. No. 27,901; J. S. Ray-Yarletts, Reg. No. 39,808; Gerald R. Woods, Reg. No. 24,144

Send all correspondence to: Jerry W. Herndon
IBM Corporation, Dept. T81/062
3039 Cornwallis Road
RTP, NC 27709
919-543-3754
FAX: 254-4330

(1) Inventor: **Kira Sterling Attwood**

Signature:



Date

2/11/2000

Residence:

1311 Pulpit Hill Road
Chapel Hill, North Carolina 27516

Citizenship:

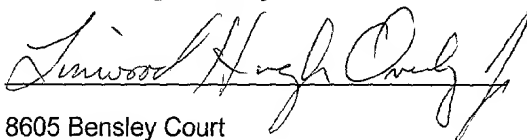
USA

Post Office
Address:

Same

(2) Inventor: **Linwood Hugh Overby, Jr.**

Signature:



Date

2/11/2000

Residence:

8605 Bensley Court
Raleigh, North Carolina 27615

Citizenship:

USA

Post Office
Address:

Same

(3) Inventor: **Chien-En Sun**

Signature:



Date

2/11/2000

Residence:

103 Chippoaks Drive
Chapel Hill, North Carolina 27514

Citizenship:

USA

Post Office
Address:

Same